UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE NEW YORK TIMES COMPANY and NEIL BEDI,

Plaintiffs,

v.

UNITED STATES DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY,

Defendant.

25 Civ. 2333 (DLC)

MEMORANDUM OF LAW IN SUPPORT OF UNITED STATES DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY'S MOTION FOR SUMMARY JUDGMENT

JAY CLAYTON
United States Attorney for the
Southern District of New York
Counsel for Defendant
86 Chambers Street, 3rd Floor
New York, New York 10007
Telephone: (212) 637-2697
peter.aronoff@usdoj.gov

Of Counsel:

PETER ARONOFF
Assistant United States Attorney

CONTENTS

AUTHORITIES

Page(s)

Cases

Statutes

Rules

PRELIMINARY STATEMENT

This Freedom of Information Act case concerns a single, two-page document—a report generated from a Defense Department database that shows any security clearances that Elon Musk held as of September 2024. Plaintiffs The New York Times Company and its reporter, Neil Bedi, requested the record in September 2024. The Defense Counterintelligence and Security Agency ("DCSA" or the "government") promptly searched for and located the document, and responded on October 2, 2024, that it was withholding it in full on privacy grounds.

This withholding was proper under FOIA exemptions 6 and 7(C). DCSA makes decisions about whether to grant security clearances after evaluating an applicant's detailed personal information, including family history, foreign travel and contacts, criminal history, finances, mental health, sexual behavior, and drug and alcohol use. As the government's declarant logically and plausibly explains, disclosing whether an individual holds security clearances—and whether any of those clearances are granted with conditions, or under a waiver—carries a substantial privacy interest, because it would reveal whether the government's investigation of these matters unearthed substantial derogatory information, and invite speculation about what that information might be. On the other side of the exemption 6 and 7(C) balance, disclosing a list of any clearances Mr. Musk held in September 2024—months before he accepted a position as a Special Government Employee—would not shed light on the only public interest that qualifies for FOIA purposes, which is the extent to which the disclosure contributes "significantly to public understanding *of the operations or activities of the government*." *DOD v. FLRA*, 510 U.S. 487, 495 (1994). Disclosure of the requested record would therefore constitute a clearly unwarranted invasion of Mr. Musk's personal privacy, or at a minimum, could reasonably be expected to constitute an unwarranted invasion of his personal privacy. It is thus properly withheld under exemptions 6 and

7(C), and the government should be granted summary judgment.

BACKGROUND

A. Background Investigations and DCSA

DCSA, an agency within the Department of Defense, is the largest provider of background investigations in the federal government. Declaration of Charles D. Watters ("Watters Decl.") ¶ 4. DCSA's work includes clearance applications for federal government employees and contractors. *Id*.

DCSA's background investigations are designed to examine each applicant as a "whole person" to determine whether the person is an acceptable security risk. Watters Decl. ¶ 13. DCSA's process is structured by guidance, known as the Security Executive Agent Directive 4 ("SEAD-4"), that applies to all executive branch agencies that adjudicate security clearance. Watters Decl. ¶ 13. Evaluating the "whole person" entails "an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk," and the agency should consider "[a]ll available, reliable information about the person, past and present, favorable and unfavorable." *Id*. (quoting SEAD-4). SEAD-4 lays out thirteen relevant topics for assessing the whole person, which cover allegiance to the United States, foreign influence or preference, sexual behavior and personal conduct, finances, alcohol and drug use, psychological conditions, criminal conduct, handling protected information, outside activities, and use of information technology. *Id*. ¶ 14.

To begin gathering relevant information, DCSA requires an individual undergoing a background investigation to complete a Questionnaire for National Security Positions ("SF-86"). *Id*. ¶ 15. As the SF-86 states, the background investigation is designed to determine whether the investigated individual is "reliable, trustworthy, of good conduct and character, and loyal to" the United States. *Id*. (quoting SF-86). The SF-86 asks for information relevant to the topics laid out

in SEAD-4, including family history, every place where the applicant has lived for the past ten years, education and employment history, foreign contacts and travel, psychological and emotional health, police record, drug and alcohol use, and finances. *Id*. Once the SF-86 is complete, the DCSA may gather additional information by interviewing the subject's friends, family, and associates. *Id*.

Once DCSA has gathered relevant information, it adjudicates the application. *Id*. ¶ 19. DCSA's adjudication decision reflects its judgment of an applicant's reliability and trustworthiness to possess and maintain access to national security information. *Id*. DSCA may grant or deny an application; or it may grant clearance subject to conditions designed to mitigate specific security concerns; or it may grant a waiver permitting access despite substantial issues if the benefit of eligibility clearly outweighs any security concerns. *See* SEAD-4 Appx. C; Watters Decl. ¶¶ 21-22.

Individuals who receive a clearance are enrolled into a continuous evaluation program called Trusted Workforce 2.0. Under this program, DCSA receives and evaluates new relevant information to ensure they continue to meet clearance requirements and should continue to hold positions of trust. *Id.* ¶ 17.

Information about security clearances is stored on a software platform called the Defense Information System for Security, or DISS. *Id*. ¶ 6. DISS is the authoritative record for eligibility determinations made by DCSA, and contains the records identifying any security clearances Mr. Musk held, as plaintiffs requested. *Id*. The specific document at issue here consists of a list of any security clearances Mr. Musk possessed as of September 2024, when the DISS search was conducted (including any conditions or waivers attached). *Id.*

B. Procedural History

In mid-September 2024, plaintiffs sent a FOIA request to DCSA seeking a list of security clearances granted to Elon Musk. Watters Decl. ¶ 5. DCSA FOIA staff familiar with the subject

matter initiated a search in the Defense Information System for Security, or DISS, a software platform for all of the Department of Defense that helps manage personnel security, including clearances for government employees and contractors. *Id*. DISS is the authoritative source documenting any determinations that DCSA makes about eligibility for accessing classified information, and contains the clearance information plaintiffs requested. *Id*. DCSA staff searched in DISS using personal identifiers for Mr. Musk. *Id*. The search yielded a single two-page document. *Id*.

On October 2, DCSA responded to plaintiffs' request by letter. *Id*. ¶ 7. The response noted that DCSA was withholding the two responsive pages in full on privacy grounds pursuant to FOIA's exemptions 6 and 7(C).

On December 15, plaintiffs filed an administrative appeal, noting Mr. Musk's high public profile and association with the then-incoming administration. *Id*. ¶ 8. DCSA denied the appeal by letter on January 27, 2025. Several days later, on February 2, plaintiffs submitted a request for reconsideration, highlighting Mr. Musk's status as a special government employee in the new Administration. *Id*. DCSA denied the reconsideration request on February 18. *Id*.

Plaintiffs filed this lawsuit on March 20. *See* Complaint, ECF No. 1.

ARGUMENT

I. Standards of Review

While FOIA generally requires disclosure of agency records, the statute recognizes "that public disclosure is not always in the public interest," *C.I.A. v. Sims,* 471 U.S. 159, 166–67 (1985), and mandates that records (or portions of records) need not be disclosed if they fall within the statute's enumerated exemptions, *Dep't of the Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 7 (2001); *see* 5 U.S.C. § 552(b). In addition, to withhold a record or portion under a FOIA exemption, the agency must determine either that disclosure would foreseeably harm an

interest protected by the exemption, or is prohibited by law. 5 U.S.C. § 552(a)(8)(i); *see Seife v. FDA*, 43 F.4th 231, 234 (2d Cir. 2022).

FOIA cases are generally resolved by summary judgment. *See, e.g.*, *Grand Cent. P'ship v. Cuomo*, 166 F.3d 473, 478 (2d Cir. 1999); *Carney v. DOJ*, 19 F.3d 807, 812 (2d Cir. 1994). Summary judgment is warranted if a movant shows "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). An agency meets this burden through declarations showing that it conducted a reasonable search[1] and that any asserted exemptions are justified. *Carney*, 19 F.3d at 812 (footnote omitted). The agency's declaration is "accorded a presumption of good faith." *Id.* (quotation marks omitted); *Wilner v. NSA*, 592 F.3d 60, 69 (2d Cir. 2009). An agency's explanation for the application of exemptions is sufficient if it is "reasonably detailed," *Carney*, 19 F.3d at 812, and appears logical and plausible. *See ACLU v. DOD*, 901 F.3d 125, 133 (2d Cir. 2018) (as amended Aug. 22, 2018).

II. The Government Properly Withheld the Record Under Exemptions 6 and 7(C)

The government's declarant, Mr. Watters, logically and plausibly explains, in reasonable detail, that DCSA properly withheld the two-page document in full under FOIA's privacy exemptions.

A. Legal Standards for FOIA's Privacy Exemptions

Exemption 6 exempts from disclosure information from personnel, medical, or other similar files where disclosure "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Congress intended exemption 6 to be read broadly—it encompasses any "personal information identifiable to a particular person." *Cook v. NARA*, 758

[1] Based on a discussion with plaintiffs' counsel about how the search was conducted, we understand plaintiffs do not contest the adequacy of the government's search for the two pages at issue here.

F.3d 168, 175 (2d Cir. 2014). The statute's reference to personnel, medical, and "similar" files in § 552(b)(6) is not limiting; instead, Congress intended the language to have "a broad, rather than a narrow, meaning," *State v. Washington Post Co.*, 456 U.S. 595, 600 (1982).

Exemption 7(C) protects from disclosure "records or information compiled for law enforcement purposes" whose release "could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C). "Exemption 7(C) is more protective of privacy than Exemption 6 and thus establishes a lower bar for withholding material." *ACLU v. DOJ*, 655 F.3d 1, 6 (D.C. Cir. 2011) (quotation marks omitted)).

Both of FOIA's privacy exemptions apply to any information in which a person has a more than de minimis privacy interest, unless outweighed by a cognizable public interest in disclosure. *Associated Press v. DOD*, 554 F.3d 274, 286 (2d Cir. 2009). Under both exemptions, once a protected privacy interest is found, the Court must balance the individual's privacy interest against the public's need for the information at issue. *See Wood v. FBI*, 432 F.3d 78, 86 (2d Cir. 2005). But there is only one "relevant public interest in disclosure" that the Court must weigh: "the extent to which disclosure would serve the core purpose of FOIA, which is contribut[ing] *significantly* to public understanding *of the operations or activities of the government*." *DOD v. FLRA*, 510 U.S. 487, 495 (1994) (first emphasis added). Given the importance of individual privacy rights protected by exemption 7(C) in particular, a requester "must show that the public interest sought to be advanced is a significant one, an interest more specific than having the information for its own sake," and that the requested information "is likely to advance that interest." *Nat'l Archives & Recs. Admin. v. Favish*, 541 U.S. 157, 172 (2004).

B. Application

The two-page record was properly withheld under exemptions 6 and 7(C) because disclosure would constitute a clearly unwarranted invasion of personal privacy, or at a minimum, could reasonably be expected to constitute an unwarranted invasion of personal privacy.

1. The record was compiled for a law enforcement purpose

First, the record—which was created as part of DCSA's mission to carry out background checks and adjudicate security clearance applications—was "compiled for law enforcement purposes," 5 U.S.C. § 552(b)(7), satisfying the threshold requirement for exemption 7.

Courts in this district take a practical approach based on an ordinary understanding of what constitutes "law enforcement purposes." *See generally Human Rights Watch v. Dep't of Justice Fed. Bureau of Prisons*, No. 13 Civ. 7360 (JPO), 2015 WL 5459713, at *5-6 (S.D.N.Y. Sept. 16, 2015) (surveying the law), *reconsidered in part on other grounds*, 2016 WL 3541549 (S.D.N.Y. June 23, 2016). To qualify, "an agency must establish a rational nexus between the agency's activity in compiling the documents and its law enforcement duties." *Brennan Ctr. for Justice at New York Univ. Sch. of Law v. Dep't of Homeland Sec.*, 331 F. Supp. 3d 74, 97 (S.D.N.Y. 2018). Law enforcement includes prospective efforts to prevent criminal activity and maintain security, not just efforts to investigate or prosecute past violations. *Id*. Efforts to maintain national security meet the exemption 7 threshold even apart from any civil or criminal enforcement. *See, e.g.*, *Milner v. Dep't of Navy*, 562 U.S. 562, 583 (2011) (Alito, J., concurring) (explaining that "law enforcement includes not just the investigation and prosecution of offenses that have already been committed, but also proactive steps designed to prevent criminal activity and to maintain security," including efforts to prevent terrorism).

Here, Mr. Watters confirms that the records were compiled for law enforcement purposes because they were compiled to protect national security. Watters Decl. ¶ 10. A core function of

the personnel vetting process conducted by DCSA is to prevent malign actors from obtaining security clearances. *Id*. Allowing such individuals access could risk security breaches, undermining U.S. national security—by, for example, allowing individuals to sell sensitive technology or disclose intelligence sources to an adversary. *Id*. Indeed, Executive Order 13,526, which sets the standards for classification, specifies that information may only be classified if its "unauthorized disclosure . . . reasonably could be expected to result in damage to the national security." *Id*. § 1.1(a)(4). And under certain circumstances, unauthorized disclosure of classified information may constitute a crime. *See*, *e.g.,* 18 U.S.C. § 792 *et seq*.; 50 U.S.C. § 783. Background investigations are intended in part to prevent such criminal disclosures. Watters Decl. ¶ 10.

Courts have therefore repeatedly recognized that conducting background investigations "inherently" relates to law enforcement. *Morley v. CIA*, 508 F.3d 1108, 1128-29 (D.C. Cir. 2007). With respect to security clearances in particular, agencies have a "responsibility to prevent potential bad actors from obtaining security clearances," which could allow "access to government technologies and facilities," risking a security breach. *Henderson v. ODNI*, 151 F. Supp. 3d 170, 177 (D.D.C. 2016). This meets the exemption 7 threshold. *See also Stein v. CIA*, 454 F. Supp. 3d 1, 27-28 (D.D.C. 2020) (information relating to security clearance investigations for high-level officials satisfied the law enforcement threshold requirement); *Mittleman v. OPM*, 76 F.3d 1240, 1241-43 (D.C. Cir. 1996).

2. The record carries a more than de minimis privacy interest

The withheld record—which consists principally of a list of any security clearances Mr. Musk held as of the date of the search in September 2024, Watters Decl. ¶ 6—implicates more than a de minimis privacy interest, meeting the first requirement of exemptions 6 and 7(C).

DCSA bases its security clearance adjudications on a wide range of personal information,

including the detailed personal information gathered from the applicant's completed SF-86 and further interviews with friends, family, and associates. Watters Decl. ¶¶ 15-19. The ability or inability to obtain clearances "reflects the government's judgment of an applicant's reliability and trustworthiness to possess and maintain access to national security information." Watters Decl. ¶ 15. The request here does not seek the underlying investigative file itself, but, as Mr. Watters explains, "revealing whether the DCSA granted or denied clearances (or granted them with conditions or a waiver) would shed light on" the private information contained in the investigative file, "and would invite speculation about the more detailed contents of the DCSA's investigation." *Id*. Disclosing whether an individual holds a clearance, or holds it with conditions or a waiver, gives rise to a substantial privacy interest in several ways.

First, disclosure would reveal whether the person had an active clearance or not. If the public expects the person would have a clearance, but DCSA discloses that the person in fact does not, this would likely indicate that DCSA had uncovered significant derogatory information. Watters Decl. ¶ 20. For example, if an individual is in a government or contractor position where obtaining a security clearance would be common or necessary, disclosing that the person lacked a clearance would suggest that DCSA had either denied an application or revoked access. *Id*. A denial or revocation would reveal that DCSA's investigation (or additional information learned through continuous vetting) had uncovered derogatory information of sufficient weight that a denial or revocation was warranted. *Id*. This disclosure would invite speculation and draw unwanted public attention. *Id*.

Second, disclosing the withheld information here would also disclose whether any security clearances were granted with conditions. Any such conditions also carry a substantial privacy interest. Pursuant to the SEAD-4, DCSA may determine that a certain type of clearance may be

granted only with conditions attached to it that mitigate specific concerns identified during the investigative process. Watters Decl. ¶ 21. For example, an individual might be required to submit regular financial statements if a concern is raised about finances, or might have restrictions on access to specific types of information (for example, information about a particular country where the person has close familial or other connections). *Id*. Revealing such conditions, or even the fact that the grant was conditional, would reveal private information and invite speculation about the reasons for the conditions' imposition. *Id*.

Similar reasoning applies to disclosure of whether a clearance was granted with a waiver. Under the SEAD-4, DCSA may grant a clearance "despite the presence of substantial issue information that would normally preclude eligibility," but "only when the benefit" of access "clearly outweighs any security concerns." Watters Decl. ¶ 22 (quoting SEAD-4 Appx. C). Revealing that a person obtained a clearance with a waiver would reveal that DCSA's investigation had found substantial derogatory information, inviting speculation and unwanted attention. *Id*.

For these reasons, DCSA concluded that revealing whether Mr. Musk had any security clearances—and whether any such clearances were granted conditionally, or with waivers—carries a substantial privacy interest.

Indeed, as the agency explains, it is DCSA's regular practice and policy to withhold such information under FOIA's privacy exemptions whenever it receives a third-party request for information about an individual's status and types of security clearances. Watters Decl. ¶ 23. It is insufficient to protect individual privacy for DCSA to withhold only information that clearly shows the presence of derogatory information, such as grants with conditions or waivers. *Id.* If DCSA withheld only that information, but disclosed information showing simple grants of clearances, FOIA requesters could determine based on the withholding decision whether a given individual's

records contained derogatory information. *Id.* In this way, as DCSA explains, DCSA's policy is akin to a Glomar response. *Id*.; *see Wilner*, 592 F.3d at 69-70 (explaining and approving Glomar responses to FOIA requests when acknowledging the existence or nonexistence of responsive records would itself reveal information protected by a FOIA exemption).

Courts have approved analogous Glomar-type reasoning regarding similar information. For example, in *Stein v. CIA*, No. CV 17-189 (TSC), 2024 WL 4298757, at *2 (D.D.C. Sept. 26, 2024), the court approved the withholding of information from former Secretary of State Rex Tillerson's clearance application, including information that would reveal the extent to which investigators viewed the applicant as a security risk. In deciding the issue, the court reasoned:

> Notably, the range of sensitive information that *could be* in those fields is as important as the information *actually in* former Secretary of State Tillerson's application (if any). If State only redacted the fields when that kind of sensitive information was present, the fact of redaction itself would confirm the information's presence.

Id. at *2. Similarly here, DCSA applies a consistent policy of withholding security clearance information because, if it only withheld or redacted records reflecting denials, conditions, or waivers, that withholding or redaction would itself confirm the presence of derogatory information.

3. Mr. Musk's substantial privacy interests outweigh any public interest in disclosure

Having correctly determined that the withheld information carries substantial privacy interests, DCSA properly withheld it because those privacy interests outweighed any cognizable public interest in disclosure. Disclosure of Mr. Musk's security clearance information from the fall of 2024—when Mr. Musk was a private citizen—would not "contribute significantly to public understanding of *the operation or activities of the government*." *DOD v. FLRA*, 510 U.S. at 495; Watters Decl. ¶ 27.

As an initial matter, the specific records sought here would shed little light on the most straightforward public interest that might attach—the public's ability to understand DCSA's operations or activities. As Mr. Watters explains, disclosing the list of security clearances that any one individual has received would show little about DCSA's performance of its duties. Watters Decl. ¶ 26. The withheld information would not give any meaningful insight into matters such as the thoroughness of DCSA's investigation, the fairness and accuracy of its adjudication, or its response to any new information. *Id*.

Nor does the withheld information carry a qualifying public interest in relation to Mr. Musk's activities. The request was made in September of 2024. Watters Decl. ¶ 5. DCSA promptly completed its search and responded by letter on October 2, 2024. *Id*. ¶¶ 6-7. Thus, the records at issue here were gathered more than a month before the 2024 presidential election, and they predate Mr. Musk's government employment by several months.

To be sure, it is undisputed that Mr. Musk was in the fall of 2024 (and remains today) the head of SpaceX, a government contractor. *See* ECF No. 1-2 at 1; Watters Decl. ¶ 27. In its administrative appeal, plaintiffs argued that Mr. Musk's position as a contractor gives him access to important information about spy satellites and other national security assets; grants him significant geopolitical influence; and could make him the subject of foreign influence efforts. Watters Decl. ¶ 28. As Mr. Watters explains, however, even if these topics could be connected to a qualifying public interest, disclosing the record at issue here would add little to the public's understanding of them. *Id*. Disclosing a list of Mr. Musk's security clearances would not reveal what information (if any) Mr. Musk has accessed, or reveal anything about his geopolitical influence or any foreign efforts to influence him, *id*., much less tie any of this to an activity of the United States government.

When seeking reconsideration, plaintiffs also argued that Mr. Musk's later status as an SGE tipped the balance toward disclosure. Watters Decl. ¶ 29. Specifically, plaintiffs argued, without citation, that Mr. Musk had "access[ed] highly sensitive and classified government records and systems," and that "[t]he public has an obvious interest in understanding what clearances DCSA has granted to him and exercising democratic oversight of the effectiveness of the DCSA vetting and oversight process." *Id*. (citing ECF No. 1-4 at 2). But, as Mr. Watters notes, the records at issue were generated in late September of 2024, before Mr. Musk became an SGE. *Id*.

In any event, conjecture about what information Mr. Musk may have accessed cannot constitute a qualifying public interest. When privacy rights are at stake, a requester cannot show a public interest simply by speculating that the records would expose government impropriety or negligence. *See Favish*, 541 U.S. at 172-74. Rather, it "must produce evidence that would warrant a belief by a reasonable person that the alleged Government impropriety might have occurred." *Id*. at 174. Plaintiffs have not provided evidence of any government misconduct that could support a cognizable public interest here. Watters Decl. ¶ 29.

Finally, as noted above, DCSA has a general policy and practice of not disclosing individuals' security clearance information. Watters Decl. ¶ 23. It would not be possible for DCSA to maintain this general policy, and protect the privacy interests of all the individuals with records in DISS, if it made exceptions for individuals who are "public figures," as plaintiffs have suggested is appropriate. *See* ECF No. 1-2 at 1. Being in the public eye does not eliminate FOIA's privacy exemptions. *Archibald v. U.S. Dep't of Just.*, 950 F. Supp. 2d 80, 84 (D.D.C. 2013) ("FOIA is not designed to allow the citizenry unfettered access to the private affairs of other citizens, however famous they may be.").

When seeking reconsideration of DCSA's administrative denial, plaintiffs cited *WP Co. LLC v. DOD*, 626 F. Supp. 3d 69, 82 (D.D.C. 2022) ("*Post*"), but that case does not undermine the government's assertion of FOIA's privacy exemptions here. The Washington Post sought records from multiple Defense and State Department components about former U.S. government officials' applications to work for foreign governments, which under the Constitution's Foreign Emoluments Clause require Congressional approval (which has been delegated to the Secretary of the relevant departments). *Id*. at 75. The military components withheld information about individuals on privacy grounds, including the names of lower-ranking officials, and the pay and security clearances of all officials (although the Navy released security clearances for higher-ranking officials). *Id*. at 77. Evaluating exemption 6, the court held that security clearance information was not protected. *Id*. at 82.

Post is distinguishable from this matter. First, the *Post* court held the privacy interests were relatively attenuated, finding it was "reasonable to assume that security clearances are generally correlated with rank"; the information was related to official duties, and not "personal"; and the government had not shown why disclosure could "embarrass or invite unwarranted intrusions" of the former officials' privacy. *Id*. By contrast here, DCSA has logically and plausibly explained the privacy interest in nondisclosure of any security clearances Mr. Musk held (including whether with a waiver or conditions) in September of 2024, when he was a private individual who had not served in government. Watters Decl. ¶¶ 12-23. Disclosure would reveal whether DCSA had found derogatory information during its investigation, which could invite embarrassment or speculation, *id*. ¶¶ 19-22, precisely the showing that the *Post* court found lacking in that case.

Second, the *Post* court found a significant public interest in "knowing the extent to which an applicant's security clearance is a factor in approving or rejecting foreign employment." 626 F.

Supp. 3d at 82. Here, by contrast, plaintiffs have not identified any further government action that clearances purportedly relate to. Thus, the public interest in information withheld here is minimal: it does not shed light on DCSA's own operations, and it predates Mr. Musk's government service. Watters Decl. ¶¶ 26-29. Nor, in contrast to the *Post* case, is there any inconsistent determination between government agencies. *See* 626 F. Supp. 3d at 82 (noting that the Navy had released clearances for higher-ranking former officials, while the Army and Air Force had withheld them). Rather, as Mr. Watters explains, DCSA has a uniform practice of withholding information of the type sought here, in a manner similar to a Glomar response. Watters Decl. ¶ 23.

In sum, then, DCSA properly determined that the cognizable public interest in the records was "minimal, at best, and does not outweigh Mr. Musk's privacy interests in the withheld information." Watters Decl. ¶ 30. The withheld information would shed little or no light either on DCSA's own operations, or on Mr. Musk's duties as an SGE. *Id*. It was thus proper to withhold the information under exemptions 6 and 7(C), since disclosure would constitute a clearly unwarranted invasion of his personal privacy, or at a minimum, could reasonably be expected to constitute an unwarranted invasion of personal privacy. *Id*.

III. The Government Has Disclosed All Reasonably Segregable, Non-Exempt Information

FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). An agency is "entitled to a presumption that [it] complied with the obligation to disclose reasonably segregable material." *Hodge v. FBI*, 703 F.3d 575, 582 (D.C. Cir. 2013) (quotation marks omitted). Here, Mr. Watters attests that the agency conducted a line-by-line review, but that no meaningful information could reasonably be segregated from the two withheld pages without disclosing exempt information. Watters Decl. ¶ 32.

IV. The Agencies Reasonably Foresee That Disclosure Would Harm the Privacy Interests Protected by Exemptions 6 and 7(C)

In addition to showing that the requirements of a FOIA exemption are met, an agency may not withhold information under an exemption unless it "reasonably foresees that disclosure would harm an interest protected by a [FOIA] exemption," or "disclosure is prohibited by law." 5 U.S.C. § 552(a)(8); *see Seife*, 43 F.4th at 241. Where the exemption itself requires a showing of harm, however, that may be sufficient to show foreseeable harm. *See, e.g.*, *Kendrick v. DEA*, No. 21-01624, 2022 WL 3681442, at *6 (D.D.C. Aug. 25, 2022) (explaining that, at least outside of exemption 5, "fulfilling the terms of exemptions . . . goes a long way to meeting the foreseeable harm requirement" (quotation marks omitted)).

Here, DCSA's declaration confirms that it reasonably foresees that release of the withheld information would harm the interests protected by exemptions 6 and 7(C), specifically, the privacy interests of Mr. Musk. Watters Decl. ¶ 31.

CONCLUSION

The government's motion for summary judgment should be granted.

Dated: May 30, 2025
New York, New York

Respectfully submitted,

JAY CLAYTON
United States Attorney
Southern District of New York

By: */s/ Peter Aronoff*
PETER ARONOFF
Assistant United States Attorney
86 Chambers Street, Third Floor
New York, New York 10007
Telephone: (212) 637-2697
E-mail: peter.aronoff@usdoj.gov

CERTIFICATE OF COMPLIANCE

I, Peter Aronoff, counsel of record for defendant, certify that this brief was prepared using Microsoft Word, and that this processing program has been applied to include all text other than what Local Rule 7.1(c) allows to be excluded in preparing the following word count. I further certify that this brief contains 4793 words.

By: */s/ Peter Aronoff*
Peter Aronoff
Assistant United States Attorney